United States Government Accountability Office

GAO

Statement for the Record
To the Subcommittee on Terrorism and Homeland Security, Committee on the Judiciary, U.S. Senate

For Release on Delivery
Expected at 10:00 a.m. EST
Tuesday, November 17, 2009

CYBERSECURITY

Continued Efforts Are Needed to Protect Information Systems from Evolving Threats

Statement of

Gregory C. Wilshusen, Director
Information Security Issues

David A. Powner, Director
Information Technology Management Issues

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **17 NOV 2009**	2. REPORT TYPE	3. DATES COVERED **00-00-2009 to 00-00-2009**

4. TITLE AND SUBTITLE
Cybersecurity: Continued Efforts Are Needed to Protect Information Systems From Evolving Threats

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
General Accountability Office,Statement for the Record to the Subcommittee on Terrorism and Homeland Security,Committee on the Judiciary, U.S. Senate ,Washington,DC

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**24**	

GAO
Accountability•Integrity•Reliability
Highlights

Highlights of GAO-10-230T, a statement to the Subcommittee on Terrorism and Homeland Security, Committee on the Judiciary, U.S. Senate

November 17, 2009

CYBERSECURITY

Continued Efforts Are Needed to Protect Information Systems from Evolving Threats

Why GAO Did This Study

Pervasive and sustained cyber attacks continue to pose a potentially devastating threat to the systems and operations of the federal government. In recent months, federal officials have cited the continued efforts of foreign nations and criminals to target government and private sector networks; terrorist groups have expressed a desire to use cyber attacks to target the United States; and press accounts have reported attacks on the Web sites of government agencies. The ever-increasing dependence of federal agencies on computerized systems to carry out essential, everyday operations can make them vulnerable to an array of cyber-based risks. Thus it is increasingly important for the federal government to have effective information security controls in place to safeguard its systems and the information they contain.

GAO was asked to provide a statement describing (1) cyber threats to federal information systems and cyber-based critical infrastructures, (2) control deficiencies at federal agencies that make these systems and infrastructures vulnerable to cyber threats, and (3) opportunities that exist for improving federal cybersecurity. In preparing this statement, GAO relied on its previously published work in this area.

View GAO-10-230T or key components.
For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov, or David A. Powner at (202) 512-9286 or pownerd@gao.gov.

What GAO Found

Cyber-based threats to federal systems and critical infrastructure are evolving and growing. These threats can be unintentional or intentional, targeted or non-targeted, and can come from a variety of sources, including criminals, terrorists, and adversarial foreign nations, as well as hackers and disgruntled employees. These potential attackers have a variety of techniques at their disposal, which can vastly enhance the reach and impact of their actions. For example, cyber attackers do not need to be physically close to their targets, their attacks can easily cross state and national borders, and cyber attackers can more easily preserve their anonymity. Further, the growing interconnectivity between information systems, the Internet, and other infrastructure presents increasing opportunities for such attacks. In addition, reports of security incidents from federal agencies are on the rise, increasing by over 200 percent from fiscal year 2006 to fiscal year 2008.

Compounding the growing number and kinds of threats, GAO—along with agencies and their inspectors general—has identified significant weaknesses in the security controls on federal information systems, resulting in pervasive vulnerabilities. These include deficiencies in the security of financial systems and information and vulnerabilities in other critical federal information systems. GAO has identified weaknesses in all major categories of information security controls at federal agencies. For example, in fiscal year 2008, weaknesses were reported in such controls at 23 of 24 major agencies. Specifically, agencies did not consistently authenticate users to prevent unauthorized access to systems; apply encryption to protect sensitive data; and log, audit, and monitor security-relevant events, among other actions. An underlying cause of these weaknesses is agencies' failure to fully or effectively implement information security programs, which entails assessing and managing risk, developing and implementing security policies and procedures, promoting security awareness and training, monitoring the adequacy of security controls, and implementing appropriate remedial actions.

Multiple opportunities exist to enhance cybersecurity. In light of weaknesses in agencies' information security controls, GAO and inspectors general have made hundreds of recommendations to improve security, many of which agencies are implementing. In addition, the White House and the Office of Management and Budget, collaborating with other agencies, have launched several initiatives aimed at improving aspects of federal cybersecurity. The Department of Homeland Security, which plays a key role in coordinating cybersecurity activities, also needs to fulfill its responsibilities, such as developing capabilities for protecting cyber-reliant critical infrastructures and implementing lessons learned from a major cyber simulation exercise. Finally, a panel of experts convened by GAO made several recommendations for improving the nation's cybersecurity strategy. Realizing these opportunities for improvement can help ensure that the federal government's systems, information, and critical cyber-reliant infrastructure are effectively protected.

Chairman Cardin and Members of the Subcommittee:

Thank you for the opportunity to submit this statement for the record for today's hearing on public and private sector efforts to prevent and disrupt terrorist cyber attacks against computer networks.

Pervasive and sustained cyber attacks against the United States continue to pose a potentially devastating impact on federal systems and operations. In February 2009, the Director of National Intelligence testified that foreign nations and criminals had targeted government and private sector networks to gain a competitive advantage and potentially disrupt or destroy them, and that terrorist groups had expressed a desire to use cyber attacks as a means to target the United States.[1] As recently as July 2009, press accounts reported that a widespread and coordinated attack over the course of several days targeted Web sites operated by major government agencies, including the Departments of Homeland Security and Defense, the Federal Aviation Administration, and the Federal Trade Commission, causing disruptions to the public availability of government information. Such attacks highlight the importance of developing a concerted response to safeguard federal information systems.

In this statement we will describe (1) cyber threats to federal information systems and cyber-based critical infrastructures, (2) control deficiencies that make these systems and infrastructures vulnerable to those threats, and (3) opportunities that exist for improving federal cybersecurity. In preparing this statement, we relied on our previous reports on federal information security. These reports contain detailed overviews of the scope and methodology we used. The work on which this statement is based was performed in accordance with generally accepted government auditing standards. Those standards require that we plan and perform audits to obtain sufficient, appropriate evidence to provide

[1] Director of National Intelligence, *Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence*, statement before the Senate Select Committee on Intelligence (Feb. 12, 2009).

a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provided a reasonable basis for our findings and conclusions based on our audit objectives.

Background

As computer technology has advanced, federal agencies have become dependent on computerized information systems to carry out their operations and to process, maintain, and report essential information. Virtually all federal operations are supported by automated systems and electronic data, and agencies would find it difficult, if not impossible, to carry out their missions, deliver services to the public, and account for their resources without these information assets. Information security is thus especially important for federal agencies to ensure the confidentiality, integrity, and availability of their information and information systems. Conversely, ineffective information security controls can result in significant risk to a broad array of government operations and assets. Examples of such risks include the following:

- Resources, such as federal payments and collections, could be lost or stolen.

- Computer resources could be used for unauthorized purposes or to launch attacks on other computer systems.

- Sensitive information, such as taxpayer data, Social Security records, medical records, intellectual property, and proprietary business information, could be inappropriately disclosed, browsed, or copied for purposes of identity theft, espionage, or other types of crime.

- Critical operations, such as those supporting critical infrastructure, national defense, and emergency services, could be disrupted.

- Data could be added, modified, or deleted for purposes of fraud, subterfuge, or disruption.

- Agency missions could be undermined by embarrassing incidents that result in diminished confidence in the ability of federal organizations to conduct operations and fulfill their responsibilities.

Federal Systems and Infrastructures Face Increasing Cyber Threats

Cyber threats to federal information systems and cyber-based critical infrastructures are evolving and growing. In September 2007, we reported that these threats can be unintentional and intentional, targeted or nontargeted, and can come from a variety of sources.[2] Unintentional threats can be caused by inattentive or untrained employees, software upgrades, maintenance procedures, and equipment failures that inadvertently disrupt systems or corrupt data. Intentional threats include both targeted and nontargeted attacks. A targeted attack is when a group or individual attacks a specific system or cyber-based critical infrastructure. A nontargeted attack occurs when the intended target of the attack is uncertain, such as when a virus, worm, or other malicious software[3] is released on the Internet with no specific target.

Government officials are concerned about attacks from individuals and groups with malicious intent, such as criminals, terrorists, and adversarial foreign nations. The Federal Bureau of Investigation has identified multiple sources of threats to our nation's critical information systems, including foreign nations engaged in espionage and information warfare, domestic criminals, hackers, virus writers, and disgruntled employees and contractors working within an organization. Table 1 summarizes those groups and types of individuals that are considered to be key sources of cyber threats to our nation's information systems and cyber infrastructures.

[2] GAO, *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain*, GAO-07-1036 (Washington, D.C.: Sept. 10, 2007).

[3] "Malware" (malicious software) is defined as programs that are designed to carry out annoying or harmful actions. They often masquerade as useful programs or are embedded into useful programs so that users are induced into activating them.

Table 1: Sources of Cyber Threats

Threat source	Description
Foreign nations	Foreign intelligence services use cyber tools as part of their information gathering and espionage activities. According to the Director of National Intelligence, a growing array of state and nonstate adversaries are increasingly targeting—for exploitation and potential disruption or destruction—information infrastructure, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries.[a]
Criminal groups	There is an increased use of cyber intrusions by criminal groups that attack systems for monetary gain.
Hackers	Hackers sometimes crack into networks for the thrill of the challenge or for bragging rights in the hacker community. While remote cracking once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus, attack tools have become more sophisticated and easier to use.
Hacktivists	Hacktivism refers to politically motivated attacks on publicly accessible Web pages or e-mail servers. These groups and individuals overload e-mail servers and hack into Web sites to send a political message.
Disgruntled insiders	The disgruntled insider, working from within an organization, is a principal source of computer crimes. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a victim system often allows them to gain unrestricted access to cause damage to the system or to steal system data. The insider threat also includes contractor personnel.
Terrorists	Terrorists seek to destroy, incapacitate, or exploit critical infrastructures to threaten national security, cause mass casualties, weaken the U.S. economy, and damage public morale and confidence. However, traditional terrorist adversaries of the United States have been less developed in their computer network capabilities than other adversaries. The Central Intelligence Agency believes terrorists will stay focused on traditional attack methods, but it anticipates growing cyber threats as a more technically competent generation enters the ranks.

Source: Federal Bureau of Investigation, unless otherwise indicated.

[a] Prepared statement of the Director of National Intelligence before the Senate Select Committee on Intelligence, February 12, 2009.

These groups and individuals have a variety of attack techniques at their disposal. Furthermore, as we have previously reported,[4] the techniques have characteristics that can vastly enhance the reach and impact of their actions, such as the following:

- Attackers do not need to be physically close to their targets to perpetrate a cyber attack.
- Technology allows actions to easily cross multiple state and national borders.

[4] GAO, *Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats*, GAO-07-705 (Washington, D.C.: June 22, 2007).

- Attacks can be carried out automatically, at high speed, and by attacking a vast number of victims at the same time.

- Attackers can more easily remain anonymous.

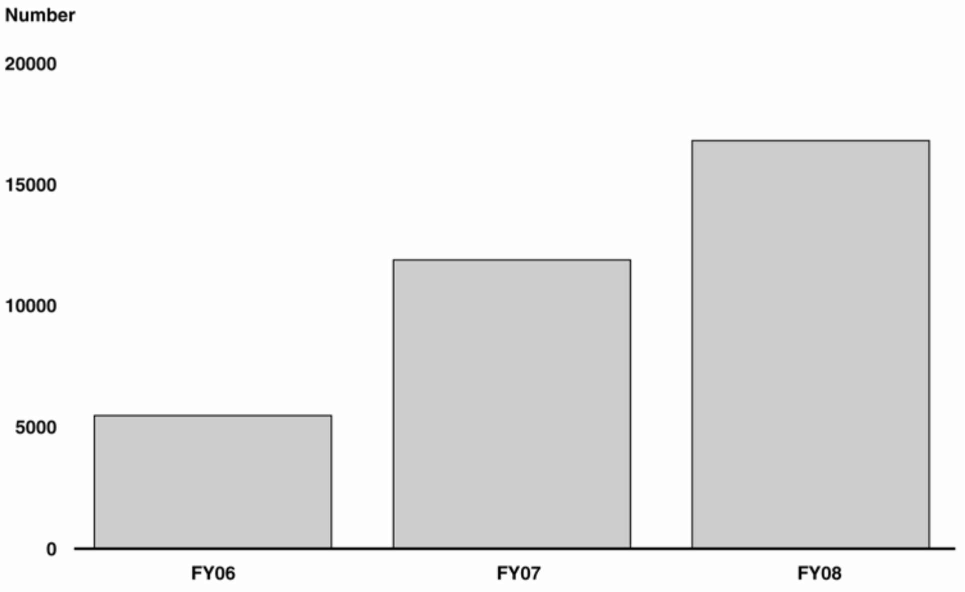
The growing connectivity between information systems, the Internet, and other infrastructures creates opportunities for attackers to disrupt telecommunications, electrical power, and other critical services. As government, private sector, and personal activities continue to move to networked operations, as digital systems add ever more capabilities, as wireless systems become more ubiquitous, and as the design, manufacture, and service of information technology have moved overseas, the threat will continue to grow. Over the past year, cyber exploitation activity has grown more sophisticated, more targeted, and more serious. For example, the Director of National Intelligence stated that, in August 2008, the Georgian national government's Web sites were disabled during hostilities with Russia, which hindered the government's ability to communicate its perspective about the conflict. The director expects disruptive cyber activities to become the norm in future political and military conflicts.

Reported Security Incidents Are on the Rise

Consistent with the evolving and growing nature of the threats to federal systems, agencies are reporting an increasing number of security incidents. These incidents put sensitive information at risk. Personally identifiable information about Americans has been lost, stolen, or improperly disclosed, thereby potentially exposing those individuals to loss of privacy, identity theft, and financial crimes. Reported attacks and unintentional incidents involving critical infrastructure systems demonstrate that a serious attack could be devastating. Agencies have experienced a wide range of incidents involving data loss or theft, computer intrusions, and privacy breaches, underscoring the need for improved security practices.

When incidents occur, agencies are to notify the federal information security incident center—the United States Computer Emergency Readiness Team (US-CERT). As shown in figure 1, the number of incidents reported by federal agencies to US-CERT has increased dramatically over the past 3 years, increasing from 5,503 incidents reported in fiscal year 2006 to 16,843 incidents in fiscal year 2008 (about a 206 percent increase).

Figure 1: Incidents Reported to US-CERT in Fiscal Years 2006 through 2008



Source: GAO analysis of US-CERT data.

The three most prevalent types of incidents reported to US-CERT during fiscal years 2006 through 2008 were unauthorized access (where an individual gains logical or physical access to a system without permission), improper usage (a violation of acceptable computing use policies), and investigation (unconfirmed incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review).

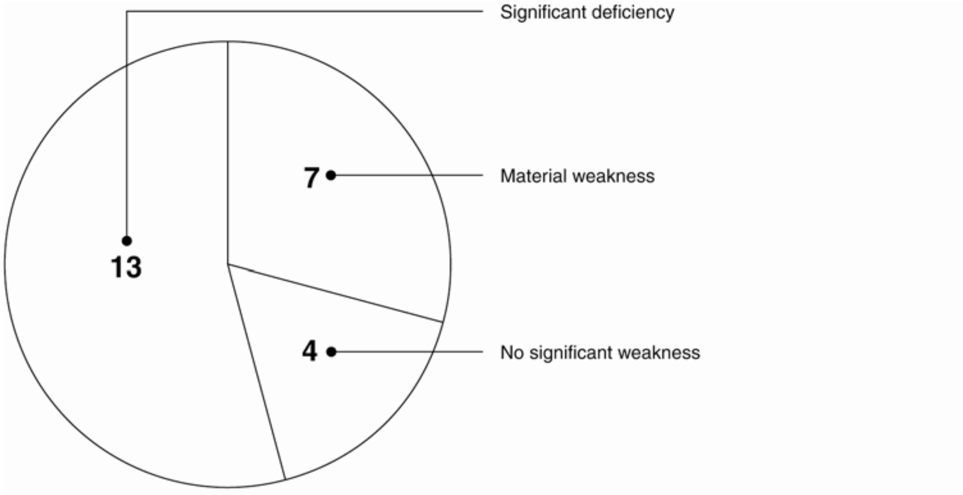
Vulnerabilities Pervade Federal Information Systems

The growing threats and increasing number of reported incidents highlight the need for effective information security policies and practices. However, serious and widespread information security control deficiencies continue to place federal assets at risk of inadvertent or deliberate misuse, financial information at risk of unauthorized modification or destruction, sensitive information at risk of inappropriate disclosure, and critical operations at risk of disruption.

In their fiscal year 2008 performance and accountability reports, 20 of 24 major agencies indicated that inadequate information system controls over financial systems and information were either a significant deficiency or a material weakness for financial statement reporting (see fig. 2).[5]

[5] A material weakness is a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected. A significant deficiency is a control deficiency, or combination of control deficiencies, that adversely affects the entity's ability to initiate, authorize, record, process, or report financial data reliably in accordance with generally accepted accounting principles such that there is more than a remote likelihood that a misstatement of the entity's financial statements that is more than inconsequential will not be prevented or detected. A control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis.

Figure 2: Number of Major Agencies Reporting Significant Deficiencies in Information Security



Source: GAO analysis of agency performance and accountability reports for FY2008.

Similarly, our audits have identified control deficiencies in both financial and nonfinancial systems, including vulnerabilities in critical federal systems. For example, we reported in September 2008[6] that, although the Los Alamos National Laboratory—one of the nation's weapons laboratories—implemented measures to enhance the information security of its unclassified network, vulnerabilities continued to exist in several critical areas. In addition, in May 2008[7] we reported that the Tennessee Valley Authority (TVA)—a federal corporation and the nation's largest public power company that generates and transmits electricity using its 52 fossil, hydro, and nuclear power plants and transmission facilities—had not fully implemented appropriate security practices to secure the control systems used to operate its critical

[6] GAO, *Information Security: Actions Needed to Better Protect Los Alamos National Laboratory's Unclassified Computer Network*, GAO-08-1001 (Washington, D.C.: Sept. 9, 2008).

[7] GAO, *Information Security: TVA Needs to Address Weaknesses in Control Systems and Networks*, GAO-08-526 (Washington, D.C.: May 21, 2008).

infrastructures. Similarly, in October 2009[8] we reported that the National Aeronautics and Space Administration (NASA)—the civilian agency that oversees U.S. aeronautical and space activities—had not always implemented appropriate controls to sufficiently protect the confidentiality, integrity, and availability of the information and systems supporting its mission directorates.

Weaknesses Persist in All Major Categories of Controls

Over the last several years, most agencies have not implemented controls sufficiently to prevent, limit, or detect unauthorized access to computer networks, systems, or information. Our analysis of inspectors general, agency, and our own reports determined that agencies did not have adequate controls in place to ensure that only authorized individuals could access or manipulate data on their systems and networks. To illustrate, weaknesses were reported in such controls at 23 of 24 major agencies for fiscal year 2008. For example, agencies did not consistently (1) identify and authenticate users to prevent unauthorized access; (2) enforce the principle of least privilege to ensure that authorized access was necessary and appropriate; (3) establish sufficient boundary protection mechanisms; (4) apply encryption to protect sensitive data on networks and portable devices; and (5) log, audit, and monitor security-relevant events. At least nine agencies also lacked effective controls to restrict physical access to information assets. We previously reported that many of the data losses occurring at federal agencies over the past few years were a result of physical thefts or improper safeguarding of systems, including laptops and other portable devices.

An underlying cause of information security weaknesses identified at federal agencies is that they have not yet fully or effectively implemented key elements for an agencywide information security program. An agencywide security program, required by the Federal Information Security Management Act (FISMA),[9] is intended to

[8] GAO, *Information Security: NASA Needs to Remedy Vulnerabilities in Key Networks*, GAO-10-4 (Washington, D.C.: Oct. 15, 2009).

[9] Federal Information Security Management Act of 2002, Title III, *E-Government Act of 2002*, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002).

provide a framework and continuing cycle of activities, including assessing and managing risk, developing and implementing security policies and procedures, promoting security awareness and training, monitoring the adequacy of the entity's computer-related controls through security tests and evaluations, and implementing remedial actions as appropriate. Our analysis determined that 23 of 24 major federal agencies had weaknesses in their agencywide information security programs.

Due to the persistent nature of these vulnerabilities and associated risks, we continued to designate information security as a governmentwide high-risk issue in our most recent biennial report to Congress,[10] a designation we have made in each report since 1997.

Opportunities Exist for Enhancing Federal Cybersecurity

Over the past several years, we and inspectors general have made hundreds of recommendations to agencies for actions necessary to resolve prior significant control deficiencies and information security program shortfalls. For example, we recommended that agencies correct specific information security deficiencies related to user identification and authentication, authorization, boundary protections, cryptography, audit and monitoring, physical security, configuration management, segregation of duties, and contingency planning. We have also recommended that agencies fully implement comprehensive, agencywide information security programs by correcting weaknesses in risk assessments, information security policies and procedures, security planning, security training, system tests and evaluations, and remedial actions. The effective implementation of these recommendations will strengthen the security posture at these agencies. Agencies have implemented or are in the process of implementing many of our recommendations.

[10] GAO, *High-Risk Series: An Update*, GAO-09-271 (Washington, D.C.: January 2009).

In June 2009[11] we proposed a list of suggested actions that could improve FISMA and its associated implementing guidance, including (1) clarifying requirements for testing and evaluating security controls; (2) requiring agency heads to provide an assurance statement on the overall adequacy and effectiveness of the agency's information security program; (3) enhancing independent annual evaluations; and (4) strengthening annual reporting mechanisms.

In addition, the White House, OMB, and certain federal agencies have undertaken several governmentwide initiatives that are intended to enhance information security at federal agencies. These key initiatives are discussed below.

- *Comprehensive National Cybersecurity Initiative:* In January 2008, President Bush began to implement a series of initiatives aimed primarily at improving the Department of Homeland Security's (DHS) and other federal agencies' efforts to protect against intrusion attempts and anticipate future threats.[12] While details of these initiatives have not been made public, the Director of National Intelligence stated that they include defensive, offensive, research and development, and counterintelligence efforts, as well as a project to improve public-private partnerships.[13]
- *The Information Systems Security Line of Business:* The goal of this initiative, led by OMB, is to improve the level of information systems security across government agencies and reduce costs by sharing common processes and functions for managing information systems security. Several agencies have been designated as service providers for computer security awareness training and FISMA reporting.

[11] GAO, *Federal Information Security Issues*, GAO-09-817R (Washington, D.C.: June 30, 2009).

[12] The White House, National Security Presidential Directive 54/ Homeland Security Presidential Directive 23 (Washington, D.C.: Jan. 8, 2008).

[13] Director of National Intelligence, *Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence*, statement before the Senate Select Committee on Intelligence (Feb. 12, 2009).

- *Federal Desktop Core Configuration:* For this initiative, OMB directed agencies that have Windows XP and/or Windows Vista operating systems deployed to adopt the security configurations developed by the National Institute of Standards and Technology, the Department of Defense, and DHS. The goal of this initiative is to improve information security and reduce overall information technology operating costs.

- *Einstein:* This is a computer network intrusion detection system that analyzes network flow information from participating federal agencies. The system is to provide a high-level perspective from which to observe potential malicious activity in computer network traffic of participating agencies' computer networks.

- *Trusted Internet Connections Initiative:* This is an effort designed to optimize individual agency network services into a common solution for the federal government. The initiative is to facilitate the reduction of external connections, including Internet points of presence.

We currently have ongoing work that addresses the status, planning, and implementation efforts of several of these initiatives.

DHS Needs to Fully Satisfy Its Cybersecurity Responsibilities

Federal law and policy[14] establish DHS as the focal point for efforts to protect our nation's computer-reliant critical infrastructures[15]—a practice known as cyber critical infrastructure protection, or cyber CIP. We have reported since 2005 that DHS has yet to fully satisfy its

[14] These include The Homeland Security Act of 2002, Homeland Security Presidential Directive-7, and the *National Strategy to Secure Cyberspace.*

[15] Critical infrastructures are systems and assets, whether physical or virtual, so vital to nations that their incapacity or destruction would have a debilitating impact on national security, national economic security, national public health or safety, or any combination of those matters. Federal policy established 18 critical infrastructure sectors: agriculture and food; banking and finance; chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; government facilities; information technology; national monuments and icons; nuclear reactors, materials and waste; postal and shipping; public health and health care; transportation systems; and water.

key responsibilities for protecting these critical infrastructures. Our reports included recommendations that are essential for DHS to address in order to fully implement its responsibilities. We summarized these recommendations into key areas listed in table 2.

Table 2: Key Cybersecurity Areas Identified by GAO

1. Bolstering cyber analysis and warning capabilities
2. Improving cybersecurity of infrastructure control systems
3. Strengthening DHS's ability to help recover from Internet disruptions
4. Reducing organizational inefficiencies
5. Completing actions identified during cyber exercises
6. Developing sector-specific plans that fully address all of the cyber-related criteria
7. Securing internal information systems

Source: GAO.

DHS has since developed and implemented certain capabilities to satisfy aspects of its responsibilities, but the department still has not fully implemented our recommendations, and thus further action needs to be taken to address these areas. For example, in July 2008, we reported[16] that DHS's US-CERT did not fully address 15 key attributes of cyber analysis and warning capabilities related to (1) monitoring network activity to detect anomalies, (2) analyzing information and investigating anomalies to determine whether they are threats, (3) warning appropriate officials with timely and actionable threat and mitigation information, and (4) responding to the threat. For example, US-CERT provided warnings by developing and distributing a wide array of notifications; however, these notifications were not consistently actionable or timely. As a result, we recommended that the department address shortfalls associated with the 15 attributes in order to fully establish a national cyber analysis and warning capability as envisioned in the national strategy. DHS agreed in large part with our recommendations.

Similarly, in September 2008, we reported that since conducting a major cyber attack exercise, called Cyber Storm, DHS had demonstrated progress in addressing eight lessons it had learned

[16] GAO, *Cyber Analysis and Warning: DHS Faces Challenges in Establishing a Comprehensive National Capability*, GAO-08-588 (Washington, D.C.: July 31, 2008).

from these efforts.[17] However, its actions to address the lessons had not been fully implemented. Specifically, while it had completed 42 of the 66 activities identified, the department had identified 16 activities as ongoing and 7 as planned for the future.[18] Consequently, we recommended that DHS schedule and complete all of the corrective activities identified in order to strengthen coordination between public and private sector participants in response to significant cyber incidents. DHS concurred with our recommendation. Since that time, DHS has continued to make progress in completing some identified activities but has yet to do so for others.

Improving the National Cybersecurity Strategy

Because the threats to federal information systems and critical infrastructure have persisted and grown, efforts have recently been undertaken by the executive branch to review the nation's cybersecurity strategy. As we previously stated, in January 2008 the Comprehensive National Cybersecurity Initiative was established with its primary aim to improve federal agencies' efforts to protect against intrusion attempts and anticipate future threats. In February 2009, President Obama directed the National Security Council and Homeland Security Council to conduct a comprehensive review to assess the United States' cybersecurity-related policies and structures. The resulting report, *"Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*,*"* recommended, among other things, appointing an official in the White House to coordinate the nation's cybersecurity policies and activities, creating a new national cybersecurity strategy, and developing a framework for cyber research and development.[19] We recently initiated a review to

[17] GAO, *Critical Infrastructure Protection: DHS Needs To Fully Address Lessons Learned from Its First Cyber Storm Exercise*, GAO-08-825 (Washington, D.C.: Sept. 9, 2008).

[18] At that time, DHS reported that one other activity had been completed, but the department was unable to provide evidence demonstrating its completion.

[19] The White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (Washington, D.C.: May 29, 2009).

assess the progress made by the executive branch in implementing the policy's recommendations.

We also testified in March 2009 on needed improvements to the nation's cybersecurity strategy.[20] In preparation for that testimony, we obtained the views of experts (by means of panel discussions) on critical aspects of the strategy, including areas for improvement. The experts, who included former federal officials, academics, and private sector executives, highlighted 12 key improvements that are, in their view, essential to improving the strategy and our national cybersecurity posture. The key strategy improvements identified by cybersecurity experts are listed in table 3.

Table 3: Key Strategy Improvement Identified by Cybersecurity Experts

1. Develop a national strategy that clearly articulates strategic objectives, goals, and priorities.
2. Establish White House responsibility and accountability for leading and overseeing national cybersecurity policy.
3. Establish a governance structure for strategy implementation.
4. Publicize and raise awareness about the seriousness of the cybersecurity problem.
5. Create an accountable, operational cybersecurity organization.
6. Focus more actions on prioritizing assets, assessing vulnerabilities, and reducing vulnerabilities than on developing additional plans.
7. Bolster public-private partnerships through an improved value proposition and use of incentives.
8. Focus greater attention on addressing the global aspects of cyberspace.
9. Improve law enforcement efforts to address malicious activities in cyberspace.
10. Place greater emphasis on cybersecurity research and development, including consideration of how to better coordinate government and private sector efforts.
11. Increase the cadre of cybersecurity professionals.
12. Make the federal government a model for cybersecurity, including using its acquisition function to enhance cybersecurity aspects of products and services.

Source: GAO analysis of opinions solicited during expert panels.

These recommended improvements to the national strategy are in large part consistent with our previous reports and extensive research and experience in this area. Until they are addressed, our

[20] GAO, *National Cybersecurity Strategy: Key Improvements Are Needed to Strengthen the Nation's Posture*, GAO-09-432T (Washington, D.C.: March 10, 2009).

nation's most critical federal and private sector cyber infrastructure remain at unnecessary risk to attack from our adversaries.

In summary, the threats to federal information systems are evolving and growing, and federal systems are not sufficiently protected to consistently thwart the threats. Unintended incidents and attacks from individuals and groups with malicious intent, such as criminals, terrorists, and adversarial foreign nations, have the potential to cause significant damage to the ability of agencies to effectively perform their missions, deliver services to constituents, and account for their resources. To help in meeting these threats, opportunities exist to improve information security throughout the federal government. The White House, OMB, and certain federal agencies have initiated efforts that are intended to strengthen the protection of federal information and information systems. In addition, the prompt and effective implementation of the hundreds of recommendations by us and by agency inspectors general to mitigate information security control deficiencies and fully implement agencywide security programs would also strengthen the protection of federal information systems, as would efforts by DHS to develop better capabilities to meets its responsibilities, and the implementation of recommended improvements to the national cybersecurity strategy. Until agencies fully and effectively implement these recommendations, federal information and systems will remain vulnerable.

Contact and Acknowledgments

If you have any questions regarding this statement, please contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov, or David A. Powner at (202) 512-9286 or pownerd@gao.gov. Other key contributors to this statement include John de Ferrari (Assistant Director), Matthew Grote, Nick Marinos, and Lee McCracken.

Related GAO Products

Information Security: NASA Needs to Remedy Vulnerabilities in Key Networks. GAO-10-4. Washington, D.C.: October 15, 2009.

Information Security: Concerted Effort Needed to Improve Federal Performance Measures. GAO-09-617. Washington, D.C.: September 14, 2009.

Information Security: Agencies Continue to Report Progress, but Need to Mitigate Persistent Weaknesses. GAO-09-546. Washington, D.C.: July 17, 2009.

Cybersecurity: Continued Federal Efforts Are Needed to Protect Critical Systems and Information. GAO-09-835T. Washington, D.C.: June 25, 2009.

Privacy and Security: Food and Drug Administration Faces Challenges in Establishing Protections for Its Postmarket Risk Analysis System. GAO-09-355. Washington, D.C.: June 1, 2009.

Aviation Security: TSA Has Completed Key Activities Associated with Implementing Secure Flight, but Additional Actions Are Needed to Mitigate Risks. GAO-09-292. Washington, D.C.: May 13, 2009.

Information Security: Cyber Threats and Vulnerabilities Place Federal Systems at Risk. GAO-09-661T. Washington, D.C.: May 5, 2009.

Freedom of Information Act: DHS Has Taken Steps to Enhance Its Program, but Opportunities Exist to Improve Efficiency and Cost-Effectiveness. GAO-09-260. Washington, D.C.: March 20, 2009.

Information Security: Securities and Exchange Commission Needs to Consistently Implement Effective Controls. GAO-09-203. Washington, D.C.: March 16, 2009.

National Cyber Security Strategy: Key Improvements Are Needed to Strengthen the Nation's Posture. GAO-09-432T. Washington, D.C.: March 10, 2009.

Information Security: Further Actions Needed to Address Risks to Bank Secrecy Act Data. GAO-09-195. Washington, D.C.: January 30, 2009.

Information Security: Continued Efforts Needed to Address Significant Weaknesses at IRS. GAO-09-136. Washington, D.C.: January 9, 2009.

Nuclear Security: Los Alamos National Laboratory Faces Challenges in Sustaining Physical and Cyber Security Improvements. GAO-08-1180T. Washington, D.C.: September 25, 2008.

Critical Infrastructure Protection: DHS Needs to Better Address Its Cyber Security Responsibilities. GAO-08-1157T. Washington, D.C.: September 16, 2008.

Critical Infrastructure Protection: DHS Needs to Fully Address Lessons Learned from Its First Cyber Storm Exercise. GAO-08-825. Washington, D.C.: September 9, 2008.

Information Security: Actions Needed to Better Protect Los Alamos National Laboratory's Unclassified Computer Network. GAO-08-1001. Washington, D.C.: September 9, 2008.

Cyber Analysis and Warning: DHS Faces Challenges in Establishing a Comprehensive National Capability. GAO-08-588. Washington, D.C.: July 31, 2008.

Information Security: Federal Agency Efforts to Encrypt Sensitive Information Are Under Way, but Work Remains. GAO-08-525. Washington, D.C.: June 27, 2008.

Information Security: FDIC Sustains Progress but Needs to Improve Configuration Management of Key Financial Systems. GAO-08-564. Washington, D.C.: May 30, 2008.

Information Security: TVA Needs to Address Weaknesses in Control Systems and Networks. GAO-08-526. Washington, D.C.: May 21, 2008.

Information Security: TVA Needs to Enhance Security of Critical Infrastructure Control Systems and Networks. GAO-08-775T. Washington, D.C.: May 21, 2008.

Information Security: Progress Reported, but Weaknesses at Federal Agencies Persist. GAO-08-571T. Washington, D.C.: March 12, 2008.

Information Security: Securities and Exchange Commission Needs to Continue to Improve Its Program. GAO-08-280. Washington, D.C.: February 29, 2008.

Information Security: Although Progress Reported, Federal Agencies Need to Resolve Significant Deficiencies. GAO-08-496T. Washington, D.C.: February 14, 2008.

Information Security: Protecting Personally Identifiable Information. GAO-08-343. Washington, D.C.: January 25, 2008.

Information Security: IRS Needs to Address Pervasive Weaknesses. GAO-08-211. Washington, D.C.: January 8, 2008.

Veterans Affairs: Sustained Management Commitment and Oversight Are Essential to Completing Information Technology Realignment and Strengthening Information Security. GAO-07-1264T. Washington, D.C.: September 26, 2007.

Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain. GAO-07-1036. Washington, D.C.: September 10, 2007.

Information Security: Sustained Management Commitment and Oversight Are Vital to Resolving Long-standing Weaknesses at the Department of Veterans Affairs. GAO-07-1019. Washington, D.C.: September 7, 2007.

Information Security: Selected Departments Need to Address Challenges in Implementing Statutory Requirements. GAO-07-528. Washington, D.C.: August 31, 2007.

Information Security: Despite Reported Progress, Federal Agencies Need to Address Persistent Weaknesses. GAO-07-837. Washington, D.C.: July 27, 2007.

Information Security: Homeland Security Needs to Immediately Address Significant Weaknesses in Systems Supporting the US-VISIT Program. GAO-07-870. Washington, D.C.: July 13, 2007.

Information Security: Homeland Security Needs to Enhance Effectiveness of Its Program. GAO-07-1003T. Washington, D.C.: June 20, 2007.

Information Security: Agencies Report Progress, but Sensitive Data Remain at Risk. GAO-07-935T. Washington, D.C.: June 7, 2007.

Information Security: Federal Deposit Insurance Corporation Needs to Sustain Progress Improving Its Program. GAO-07-351. Washington, D.C.: May 18, 2007.

(311038)

Abbreviations

DHS	Department of Homeland Security
FISMA	Federal Information Security Management Act
NASA	National Aeronautics and Space Administration
OMB	Office of Management and Budget
TVA	Tennessee Valley Authority
US-CERT	United States Computer Emergency Readiness Team

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or
TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548